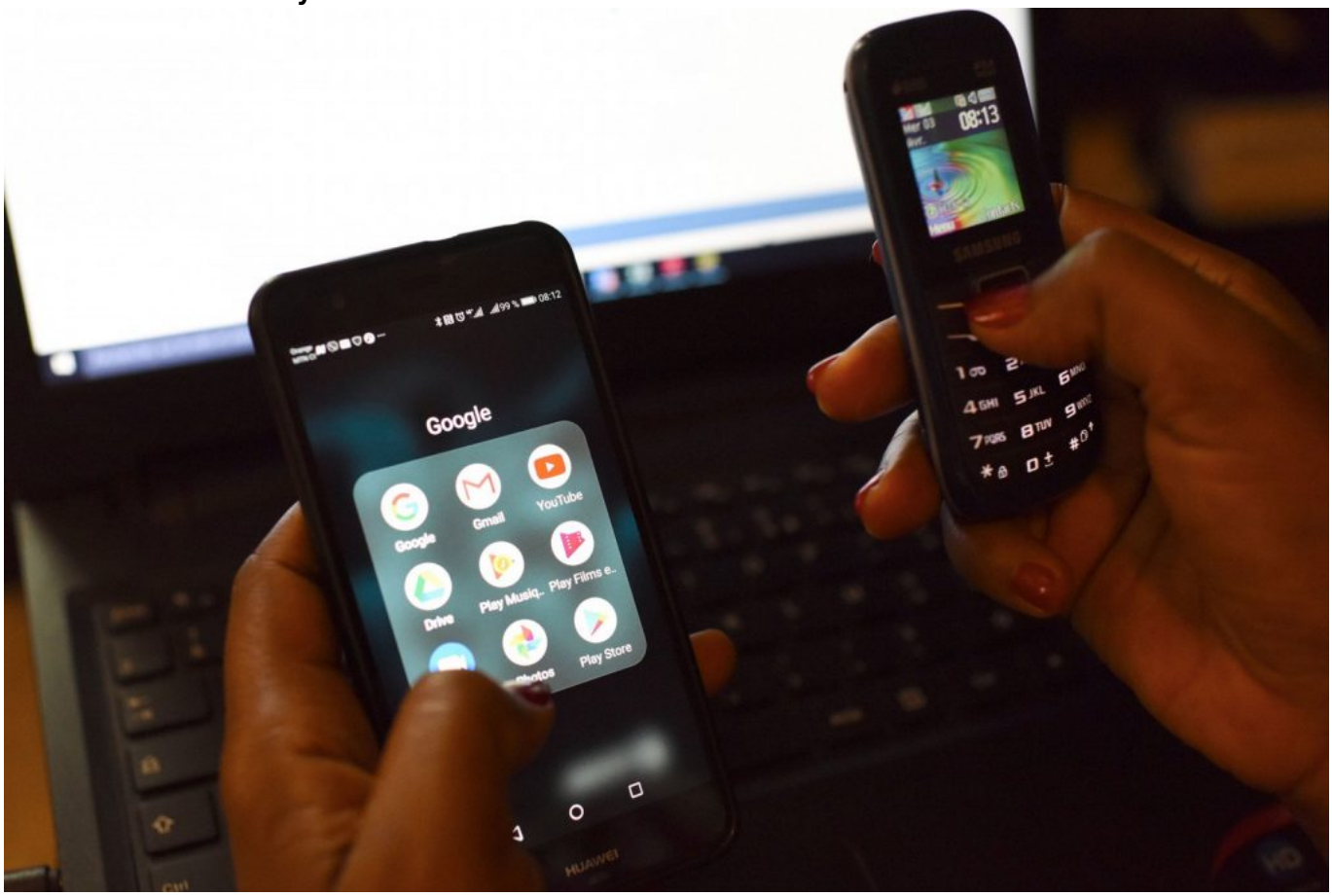
Coronavirus And Cyber Risk: The Essential Role Of The CHRO



Aon The One Brief

When it comes to cyber security, people, rather than IT systems, are often the weakest link in the chain for many organisations. And unfortunately, this link becomes even more vulnerable thanks to added risks created by the novel coronavirus (COVID-19) pandemic.

For example, the pandemic has forced many companies to move to remote working. Only 29 percent of Americans, as of 2018, were able to work from home before the pandemic, but the crisis forced organisations across industries to quickly embrace remote working, opening the door to increased cyber risk.

Many employees, unused to working from home, are more likely to handle business information on unsecure systems, or fall victim to phishing attacks that look to be from legitimate sources than they would be if they were in the office.

In addition, the economic uncertainty caused by the pandemic, as well as resulting retrenchments and changes in compensation and benefits, further heighten cyber risks. Stressed and unengaged workers are more likely to make mistakes or, in a worst-case scenario, actively take steps against their employers if they feel they have been wronged in some way.

These people risks highlight the fact that, now more than ever, cyber security isn't just the responsibility of the chief technology officer (CTO) or the chief information security officer (CISO). Increasingly, there's a role for the chief human resources officer (CHRO).

“While the CTO and CISO are, and always will be, central players in identifying and mitigating cyber risk, HR leaders need to enlist in this battle as well,” says Sam Willoughby, managing director and practice leader of investigations, Aon Cyber Solutions. “When the entire organisation prioritises and coordinates an approach to reduce cyber risk, it creates a level of collaborative resilience more powerful than single, stand-alone solutions.”

IN DEPTH

Cyber criminals quickly recognised the opportunities the COVID-19 pandemic offered. And they have found a way in to a company’s systems through either negligence or malice on behalf of the workforce. A Verizon report highlights the danger, showing that in 2019 employee actions accounted for 30 percent of all data breaches.

The result: coronavirus-related spear-phishing attacks were up 667 percent in March, according to figures from Barracuda Sentinel.

“The prevailing assumption is that cyber security is an information technology and risk management issue, but it’s more of a people issue,” says Harris Schwartz, vice president, advisory practice at Aon Cyber Solutions. “The pandemic crisis is emboldening criminals and increasing vulnerabilities. Today there’s a need for a coordinated approach, with human resources leaders helping to best address the people side of the risk. There is an exciting opportunity here for CHROs to lead in new ways.”

As companies move to remote work, bring some workers back to the office or are forced to make unpleasant personnel moves to survive the crisis, the CHRO’s role in managing pandemic risk becomes clear.

STRATEGIC TRAINING FOR A MORE SECURE REMOTE WORKFORCE

Organisations with a remote workforce face a thorny problem when it comes to reducing their exposure to cyber risk: how to strengthen defences without limiting productivity or operational flexibility. Enter the human resources team.

HR leaders can help address cyber risk by collaborating with IT to fund and launch robust education programs. For example, these programs can take the form of quarterly educational modules with real-time threat updates.

“There’s room for creativity here,” says Schwartz. “Employers might bring in outside experts as speakers or develop an office ambassador program to deliver the training. HR can lead a shift from a reliance on off-the-shelf training programs to strategic training, curricula and delivery methods.”

HR can also help ensure employees understand the organisation’s bring-your-own-device (BYOD) policies, and educate employees on responsibilities and expectations for handling confidential data or customer information.

ADDRESSING CHALLENGES WITH RETURNING TO THE OFFICE

As organisations bring all or a portion of their employees back to the workplace, they face further cyber

security challenges.

Employees will return to the office with the devices they used at home. Recent hires might have missed out on proper onboarding training before the pandemic forced offices to close or might need refresher cyber security training. And, of course, there's the possibility that a new COVID-19 outbreak might force a return to full remote working.

The HR team is well positioned to work with other areas of the organisation to help address these challenges.

As employees return, Schwartz says the HR function can:

Work with information security teams to make sure employees understand the need to have their devices screened for threats before connecting to company networks.
Ensure recent hires go through a second onboarding process where cyber security awareness features prominently.
Provide all employees returning to the workplace with updated guidance on the organisation's security policies.
Help the organisation prepare incident response plans for cyber attacks and help lead the effort to practice those plans.

Finally, the HR department can help ensure cyber security controls adapt alongside other changes to the business as the COVID-19 crisis evolves, including the possibility of future outbreaks and the need to revert quickly to remote working, Schwartz says.

MANAGING THE IMPACT OF PANDEMIC PERSONNEL MOVES

The number of cyber security incidents tied to insiders has increased by 47 percent since 2018, according to research from the Ponemon Institute. In 2020 the cost to a company from such insider attacks was expected to reach more than $11.4 million.

During the pandemic, many organisations have been forced to make difficult decisions — retrenchments, pay cuts, reductions of employee benefits — to remain economically viable.

Workers are already stressed by the pandemic's effects on all areas of their wellbeing. For some, job changes and uncertainty may breed resentment, prompting malicious activities like intellectual property theft or fraud.

HR can help address the risk in a number of ways. Frequent, clear communication can help reassure anxious employees, while managers can be trained to recognise warning signs in workers. Whistle-blower hotlines can also help address internal threats.

In addition, HR can help mitigate the threat from "bad leavers" by ensuring that off-boarding policies include deactivating access to company systems, Willoughby says.

"HR can contribute to creating a culture of compliance across the organisation through onboarding, training and development, and change management to reinforce security protocols and expectations."

IN THE CURRENT CRISIS, THE CHRO BECOMES AN ESSENTIAL CYBER SECURITY PLAYER

In the COVID-19 era, human resources leaders can play a vital role in addressing cyber risk. The CHRO can be at the centre of efforts to build cross-functional, senior leadership teams that effectively balance

the needs to address cyber security, financial risks, risk management, and legal and internal communications.

The goal is to create a culture of cyber security, and the CHRO can be a central figure in achieving that goal.

“As organisations address the impact of the pandemic, more than ever the CHRO needs to be part of the effort to prescribe and implement cyber security programs to meet 21st century demands,” Willoughby concludes.

BY *Ivan Israelstam, Chief Executive of Labour Law Management Consulting. He may be contacted on (011) 888-7944 or 0828522973 or on e-mail address: ivan@labourlawadvice.co.za. Go to: www.labourlawadvice.co.za.*